HowTo

Avira AntiVir Professional

Support

March 2010

www.avira.com

Errors in design and contents cannot be excluded
© Avira GmbH

Content

1. Setup 3

2. Configuration 11

2.1. Installing modules / uninstalling modules 11

2.2. Configuration of the Update to the Internet Update Manager 11

2.3 Configuration of Product Updates 14

2.4 Setting exceptions 14

2.4. Configuration Profiles 16

3. Creating jobs in the scheduler 19

4. Different scan profiles 21

5. Quarantine 24

6. Quick Tips 28

This document will support you to install and configure Avira AntiVir Professional in an optimal way. It contains important and helpful configuration possibilities and recommendations of the Avira Support. Also the given tips e.g. for procedures in case of virus attacks are very useful.

You will find all necessary files for installation and the manuals as PDF files ready for download on our website:

http://www.avira.com (http://www.avira.com/en/download/index.html).

1. Setup

On our website you will find two setup packages. The so-called web loader with approx. 800 KB and the complete installation package with approx. 45 MB.

1.1 Web loader

The web loader downloads all the up-to-date program files from the web servers before the installation is executed. This procedure guarantees that Avira AntiVir Professional is installed with the up-to-date virus definition files.

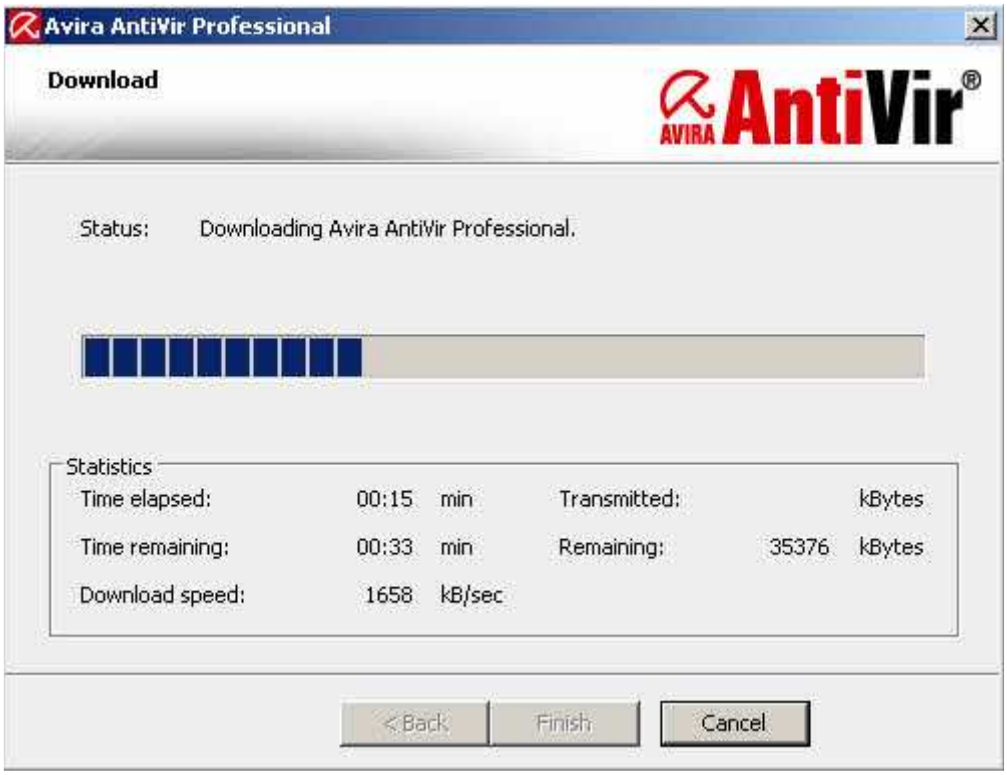
1.2 Complete Installation Package

The installation package contains the installation program as well as all necessary program files. This installation package doesn't offer a language selection for the Avira AntiVir Professional. So you have to select our English website first. On the English website the corresponding software package is offered. Here the included files might not be up-to-date.
We recommend an update immediately after the installation to make sure that all the files are up-to-date.

After having downloaded the installation files of the Avira AntiVir Professional, please, first start the installation of Avira AntiVir Professional with a double click: (avira_antivir_professional.exe or avira_antivir_professional_en.exe)

Please, click on **next** in the menu of the assistant that appears afterwards. In case you have chosen the web loader you can now select the language version you need.

Now the web loader downloads the necessary program files and virus definition files.



Afterwards you can choose a setup type:

Express:

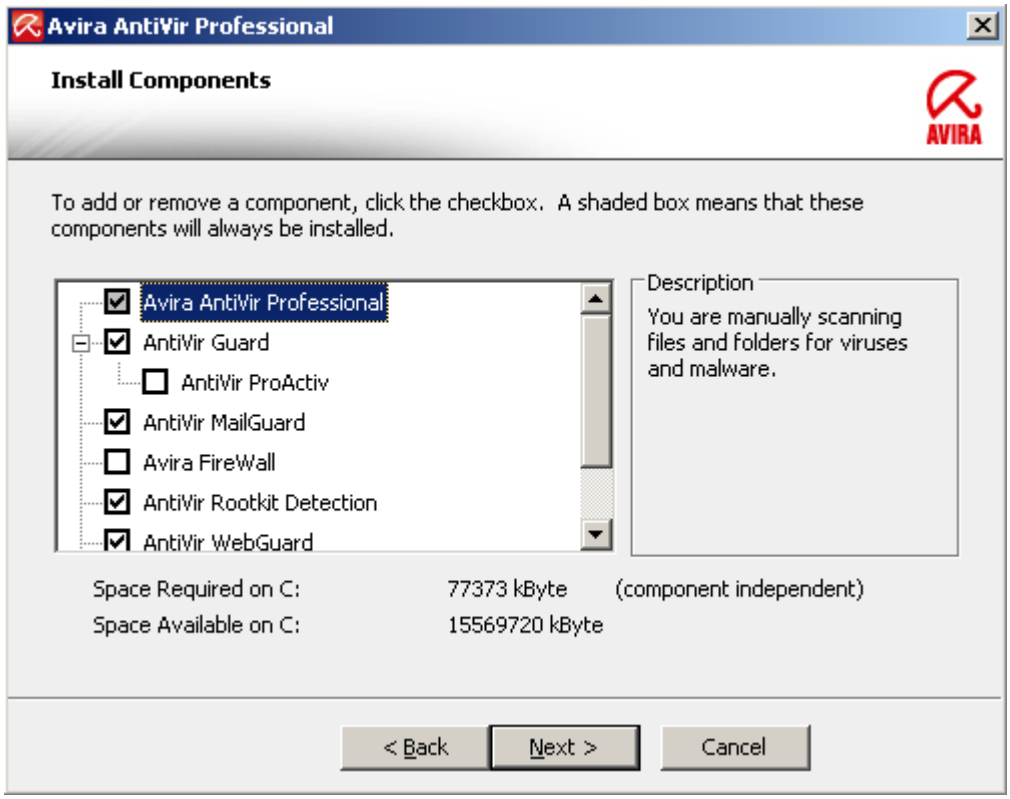
- Avira AntiVir Professional will be installed completely with all program components (modules)
- The program files are installed in the given default directory: C:\Program Files\Avira\AntiVir Desktop

Custom:

- You can choose a target folder for the program files which have to be installed
- You have the possibility to choose program components / modules for the installation
- You can deactivate the creation of a desktop icon and a program group in the start menu

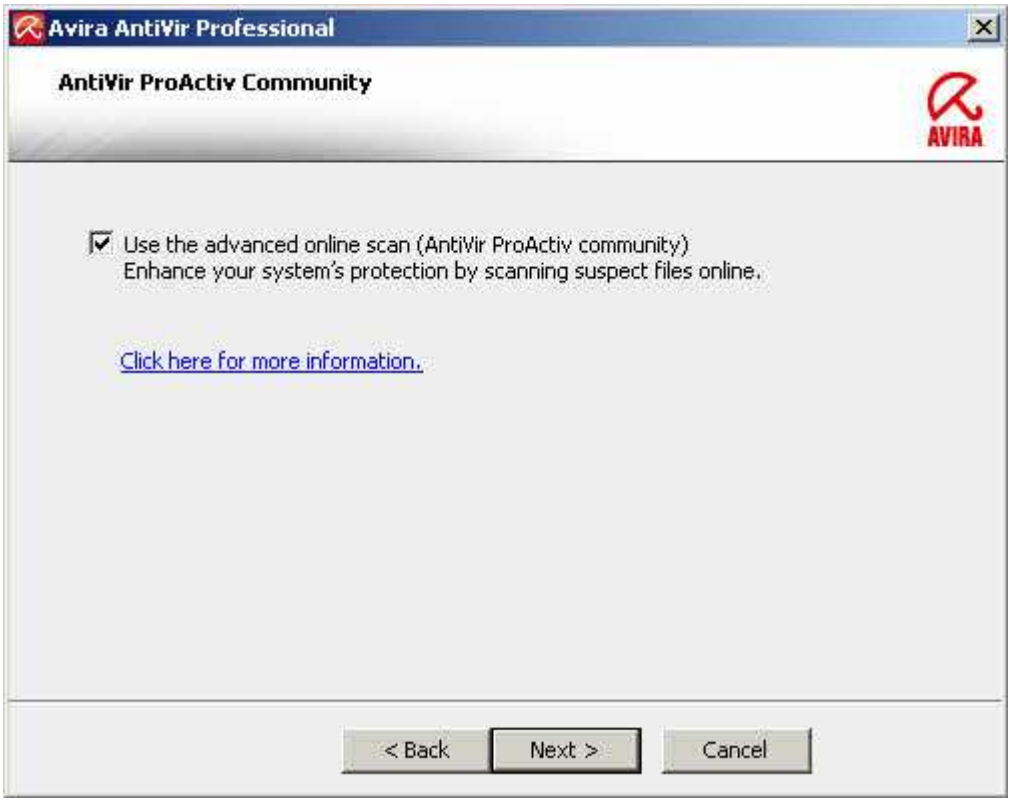
In the custom setup you can choose the following modules.

- **AntiVir Guard** (permanent scanning of all file accesses in real time)
- **AntiVir MailGuard** (permanent scanning of all incoming and outgoing emails (POP3, IMAP, SMTP) including attachments)
- **AntiVir ProAcitv** (Rule-based control over incoming and outgoing Internet traffic)
- **AntiVir WebGuard** (permanent protection against viruses and malware via browser)
- **Shell Extension** (direct scanning of files and directories in the Windows Explorer)


Avira AntiVir Professional
Install Components
AVIRA
To add or remove a component, click the checkbox. A shaded box means that these components will always be installed.
Avira AntiVir Professional
AntiVir Guard
AntiVir ProActiv
AntiVir MailGuard
Avira FireWall
AntiVir Rootkit Detection
AntiVir WebGuard
Description
You are manually scanning files and folders for viruses and malware.
Space Required on C: 77373 kByte (component independent)
Space Available on C: 15569720 kByte
< Back
Next >
Cancel

Avira AntiVir ProActiv is a new behavior based detection technology developed by Avira which is integrated from Version 10 on. ProActiv protects your computer against new and unknown malware which isn't yet detected by virus definitions and heuristics.

Avira AntiVir ProActiv monitors the system in real time and detects attacks as soon as they are started. Sensors are continuously supervising the system and look for unusual behavior. The ProActiv component uses rule sets in order to identify malicious behavior. These rule sets have been developed by the Avira Malware Research Center and are constantly provided with new data by the Avira data base.
Avira AntiVir ProActiv sends information about detected suspicious programs to the data base. You have the possibility to deactivate this data transfer to the Avira data base. In case a program shows a malicious behavior, it is treated and reported just as malware.


Avira AntiVir Professional
AntiVir ProActiv Community
AVIRA
Use the advanced online scan (AntiVir ProActiv community)
Enhance your system's protection by scanning suspect files online.
Click here for more information.
< Back
Next >
Cancel

Hint: The ProActiv Technology is not yet available for 64 bit systems. Windows 2000 is not supported.

The MailGuard is needed if you receive and send your emails via POP3, SMTP or IMAP.

You can delete the MailGuard as a module in case one of the following points is fulfilled:

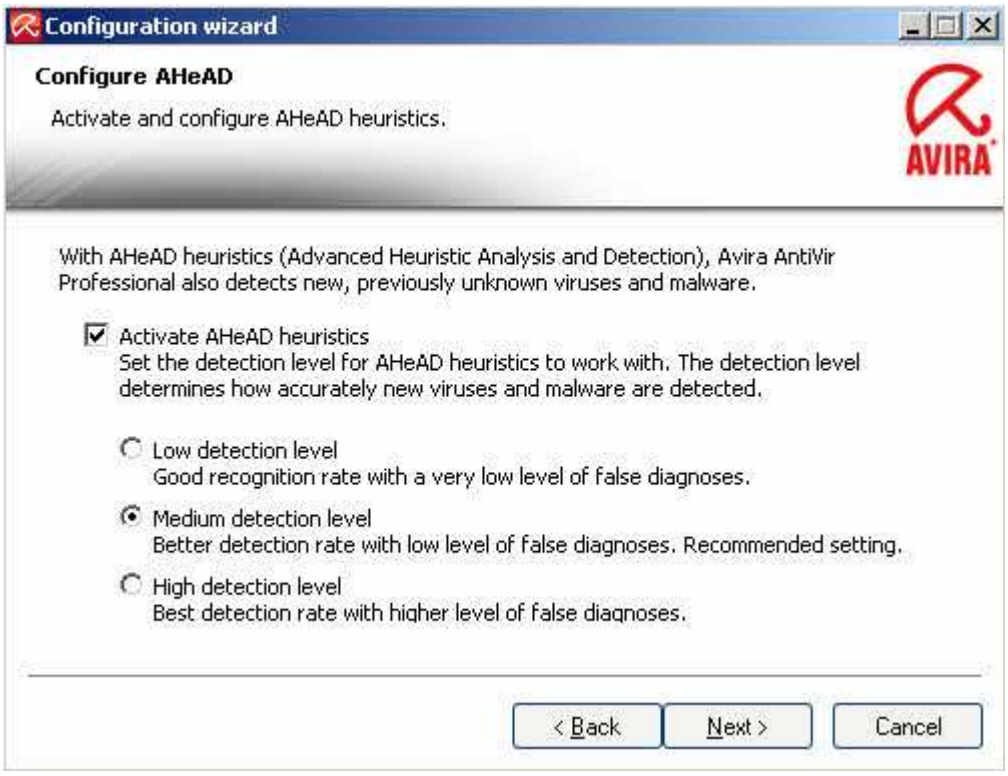
- *If you have the email traffic already scanned on an email server, e.g. by AntiVir Exchange or AntiVir MailGate*
- *If you receive emails via webaccess, that means e.g. you get your emails directly on gmx.com or web.com etc.*

You protect yourself against viruses and malware which are downloaded on your computer from websites with the WebGuard.

- *The WebGuard can be deleted as a module, if the http traffic is already scanned, e.g. by AntiVir ISA Server or AntiVir MailGate*

Afterwards the windows “Install license” appears.
Choose the directory where you have saved the license file “hbedv.key”.

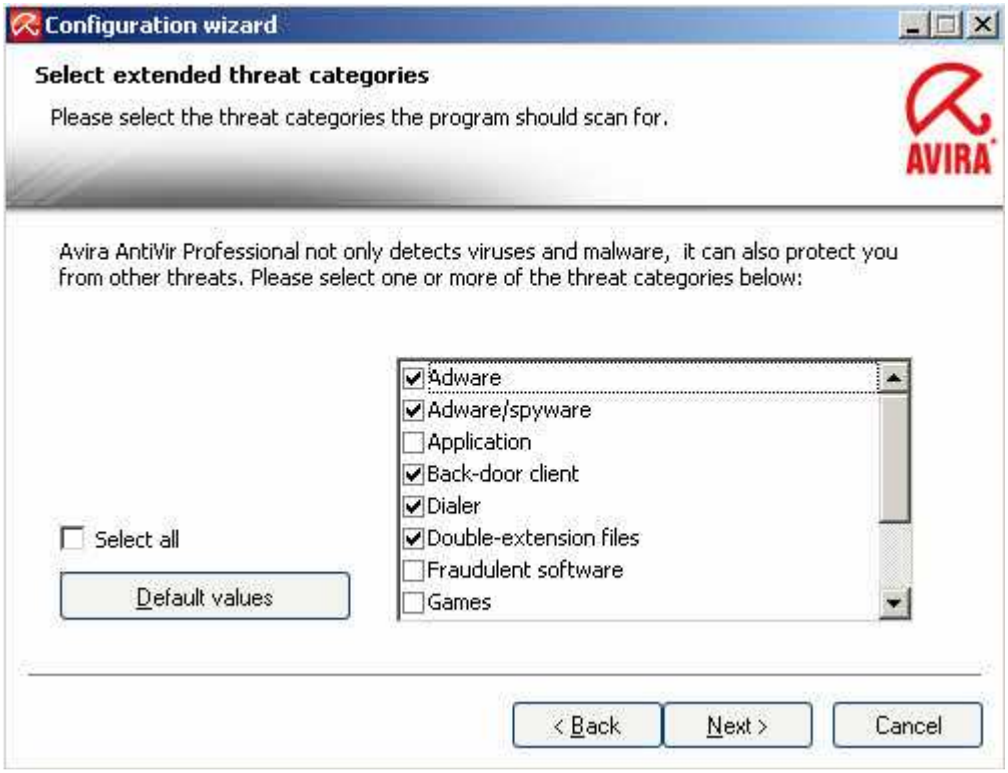
As soon as you have finished the installation, the configuration assistant appears. The assistant leads you through the basic settings of the Avira AntiVir Professional. In the next dialogue window you can configure the engine and choose the detection level for the AHeAD technology. The chosen detection level is used for the settings of the AHeAD technology of the scanner (direct scan) and of the guard (real-time scan).


Configuration wizard
Configure AHeAD
Activate and configure AHeAD heuristics.
AVIRA
With AHeAD heuristics (Advanced Heuristic Analysis and Detection), Avira AntiVir Professional also detects new, previously unknown viruses and malware.
Activate AHeAD heuristics
Set the detection level for AHeAD heuristics to work with. The detection level determines how accurately new viruses and malware are detected.
Low detection level
Good recognition rate with a very low level of false diagnoses.
Medium detection level
Better detection rate with low level of false diagnoses. Recommended setting.
High detection level
Best detection rate with higher level of false diagnoses.
< Back
Next >
Cancel

Please, be aware that a high detection level detects a large quantity of unknown malware, but it also increases the risk of false positives.

What does heuristic mean?
Heuristic is a method of detection which is able to detect unknown viruses. A profound analysis of the code looks for functions which are typical for viruses. In case the examined code has suspicious characteristics, AntiVir indicates the suspicious file. This doesn't mean that the code is really a virus, false positives are possible.

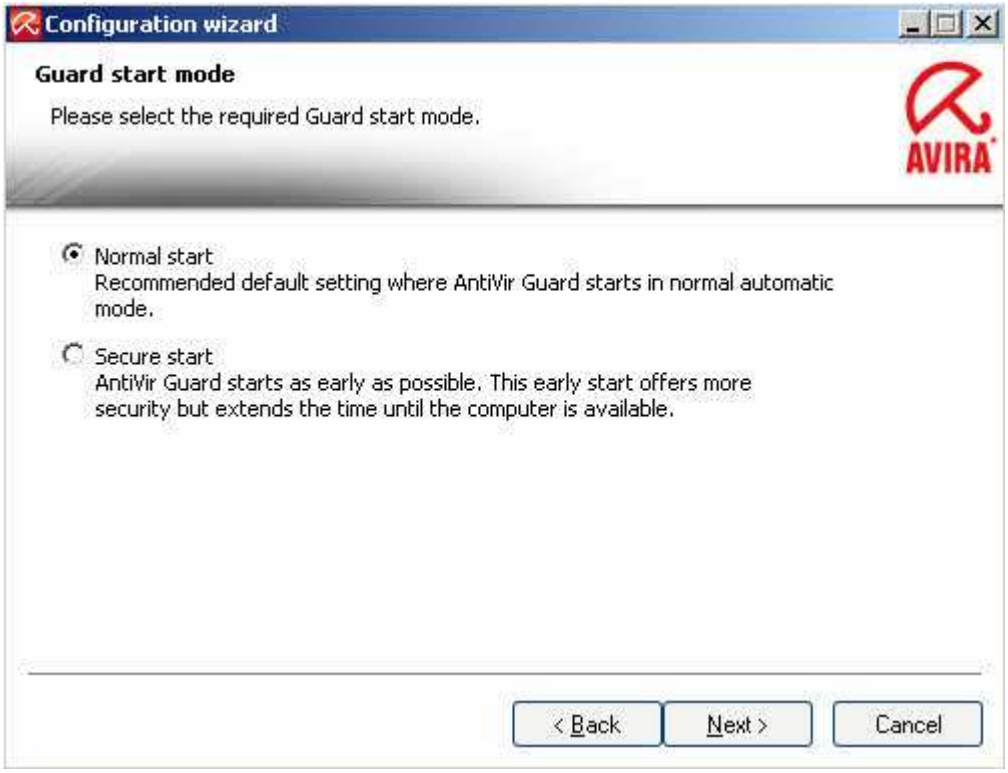
In the following menu you can choose the extended threat categories, which will be detected:



These options are activated by default as the risks of adware/spyware and back-door control software, phishing and dialers are very high. However, many administrator tools are detected by Avira as "Security Privacy Risk". AntiVir cannot distinguish if a suspicious program is used intentionally by an admin. This is why we excluded application, SPR and games from the default settings.

You can find an overview of all threat categories and their meaning in the quick tips at the end of this document.

Please, choose the start mode of the AntiVir Guard afterwards. You can choose between the normal and the safe start.


Configuration wizard
Guard start mode
Please select the required Guard start mode.
AVIRA
Normal start
Recommended default setting where AntiVir Guard starts in normal automatic mode.
Secure start
AntiVir Guard starts as early as possible. This early start offers more security but extends the time until the computer is available.
< Back
Next >
Cancel

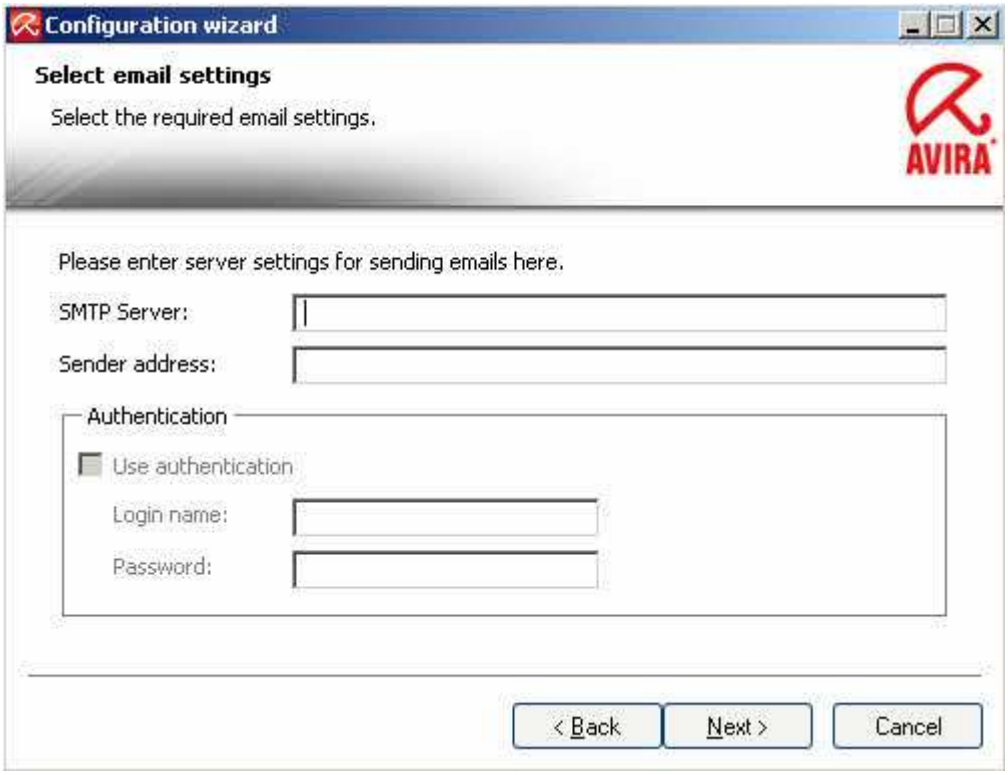
Using the “normal” start the guard gets started in the normal, automatic mode. This is the recommended start mode.

Using the “safe start” the guard is loaded as soon as possible. This increases the security level but the start needs more time.

Some viruses are loaded directly with the operation system. So they might be already active before the AntiVir Guard is loaded.

Using the safe start, the guard is started at first. Not until the guard is loaded completely and works the start of the other component is continued. So there is more time needed for the system start.
In the following configuration dialogue you can enter the server settings for the emails.

Avira AntiVir Professional forwards its emails via SMTP in order to send email alerts from the different modules, guard, scanner and updater. In case you don’t know the data of your SMTP server or you don’t want to use this option, you can leave the relevant boxes empty.



Afterwards you can choose the option “Short system scan after installation” in order to scan your computer directly after the installation.

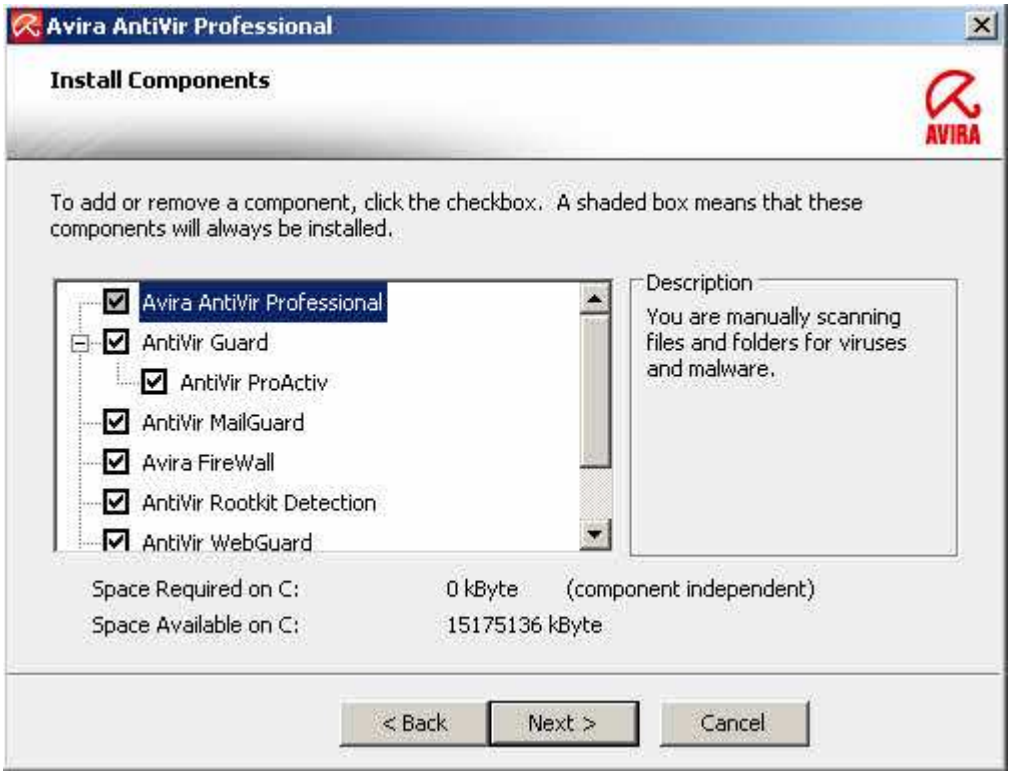
2. Configuration

2.1. Installing modules / uninstalling modules

Different modules can be chosen for the installation, added or deleted.

This might be necessary in order to save resources or to solve vulnerabilities. If you want to add or delete program components of the recent Avira AntiVir Professional installation go to the System Control, to Software. In Vista the menu is called Programs.

Choose Avira AntiVir Professional and click on *Change.* In the dialogue of the Avira AntiVir Professional, please choose the option *Change program*. You are guided through the changing installation.


Avira AntiVir Professional
Install Components
AVIRA
To add or remove a component, click the checkbox. A shaded box means that these components will always be installed.
Avira AntiVir Professional
AntiVir Guard
AntiVir ProActiv
AntiVir MailGuard
Avira FireWall
AntiVir Rootkit Detection
AntiVir WebGuard
Description
You are manually scanning files and folders for viruses and malware.
Space Required on C: 0 kByte (component independent)
Space Available on C: 15175136 kByte
< Back
Next >
Cancel

2.2. Configuration of the Update using the Internet Update Manager

In case you are using several Avira AntiVir Professional installations in the network and you want to update them centrally you can use our free-of-charge module “Internet Update Manager”. This is an option if e.g. only one computer should have access to the Internet but the virus definition files on all computers in the network should be constantly up-to-date. Furthermore, you are saving traffic and don’t burden the Internet connection unnecessarily.

You can find the tool clicking on the following link:

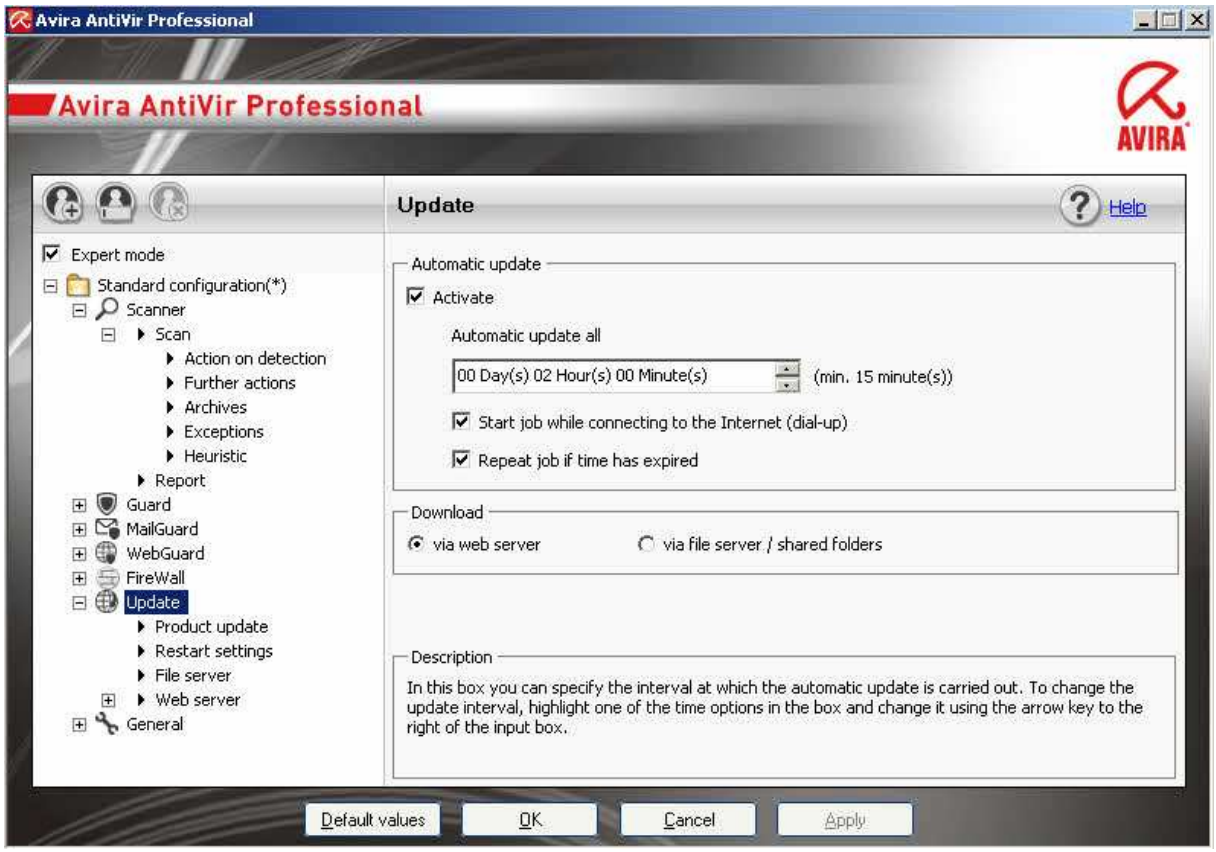
http://www.avira.de/en/downloads/avira_antivir_professional.html

You should install this software on a server operating system. For detailed information about the installation and configuration of the Internet Update Manager, please read the corresponding manual which you can download from the link mentioned above.

After the installation and configuration, the Internet Update Manager downloads the new virus definition files of the Avira AntiVir Professional due to the scheduled intervals and saves them into its root directory.
As the Internet Update Manager also provides an integrated web server with the port 7080, all workstations in the local network can get a connection to this directory and load their updates.

In order to configure the updates of the Avira AntiVir Professional, please proceed as follows:

Open the configuration of the Avira AntiVir Professional
Activate the “Expert mode”
Go to the “General” and “Update”
Choose the option “via web server”



Afterwards, please go to the point “Web server”. Here you can find two boxes, “Priority server” and “Default server”.

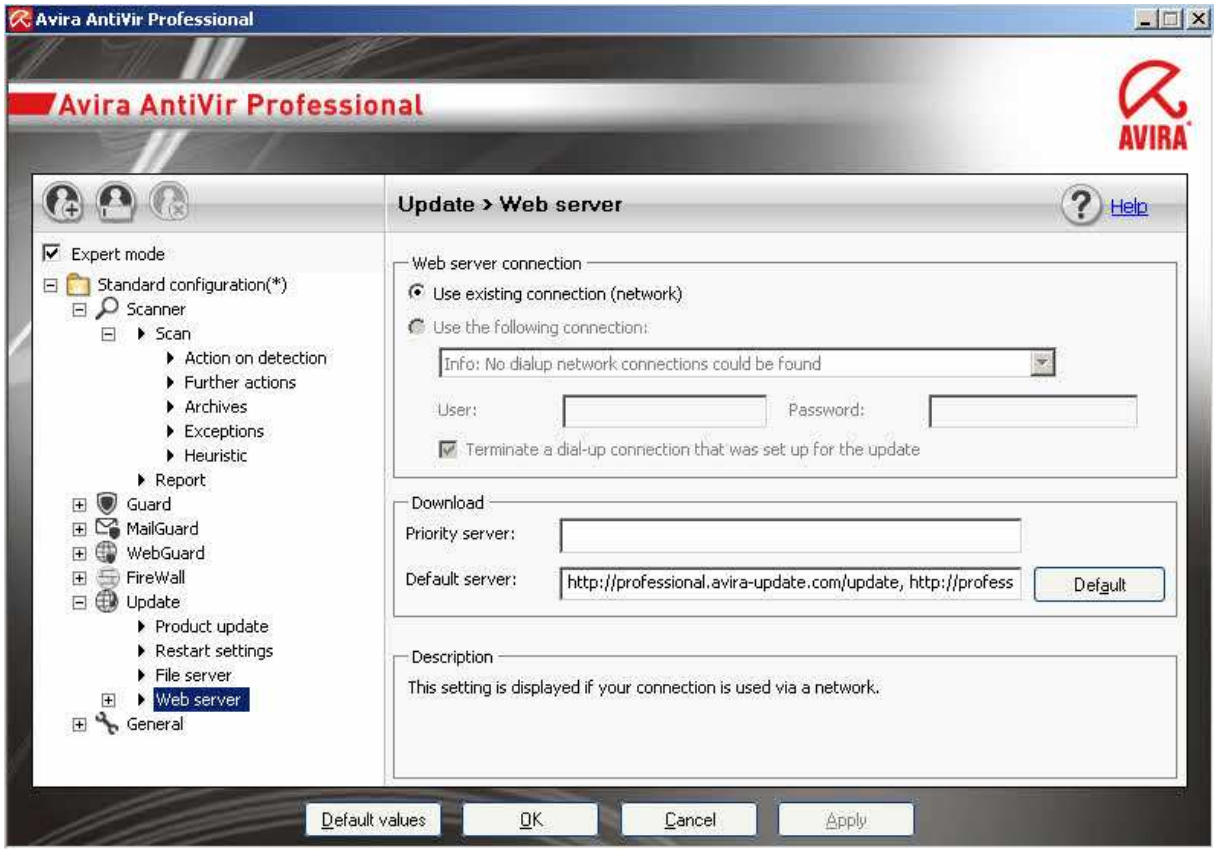
Avira AntiVir Professional tries to contact the priority server in the first place. In case there is no connection to the priority server available, AntiVir tries to get a connection to the default server.
Therefore the function “Priority server” should be used for the updates via the Internet Update Manager (IUM). This is very useful if notebooks are used in the enterprise network which have to be updated also being outside the network.

In case the IUM computer is offline, the Avira AntiVir Professional contacts the default server automatically if you have configured the priority server (IUM address) and the default server (Avira download server).

The entry you should make in this box looks is as follows:

http://[IP-Adresse of the IUM computer]:7080/update (in case of AntiVir 9 and 10)
http://[IP-Adresse of the IUM-Rechners]:7080/upd (in case of AntiVir 8)

Example:
http://192.168.0.1:7080/update
http://192.168.0.1:7080/upd



You can change the port of the Internet Update Manager if this port is already occupied in your network. Double click the navigation menu of the Internet Update Manager on the corresponding server (default setting: “local host”) → “settings” → “Networks”. Here you can change the port of the server from 7080 to the required port.

Accordingly, the settings for the update configuration of the Avira AntiVir Professional have to be changed.

It is important that the chosen path is enabled in the whole network and in each firewall of the workstations.

2.3 Configuration of Product Updates

You can find the point “product updates” in the configuration settings of the update of the Avira AntiVir Professional. Avira provides all customers with software updates in order to offer new features or to resolve problems. The setting “Download and install product updates automatically” can cause a reboot. The reboot is activated automatically by Avira AntiVir Professional in order to avoid vulnerabilities.

You can prevent an enforced reboot by choosing “Notify user if product updates are available”. You can configure this via the configuration of the Avira AntiVir Professional via the point “General” → “Update”.
After that you can plan when the product update should be installed e.g. at a moment when the PC can be rebooted without causing any inconvenience.

2.4 Setting exceptions

Avira AntiVir Professional is connected directly to the operating system. Especially the Avira AntiVir Guard scans all files during the real-time scan at each write or read access. It is therefore recommended to exclude special programs and their processes from the AntiVir scan.

For example all programs which operate with a database in the background are concerned like accounting programs or financial software

Furthermore special backup programs which require a data backup of your systems are concerned. During a backup a read access is made of all files of the computer and the guard constantly scans each file which is saved by the backup program. This can affect the performance of your computer.

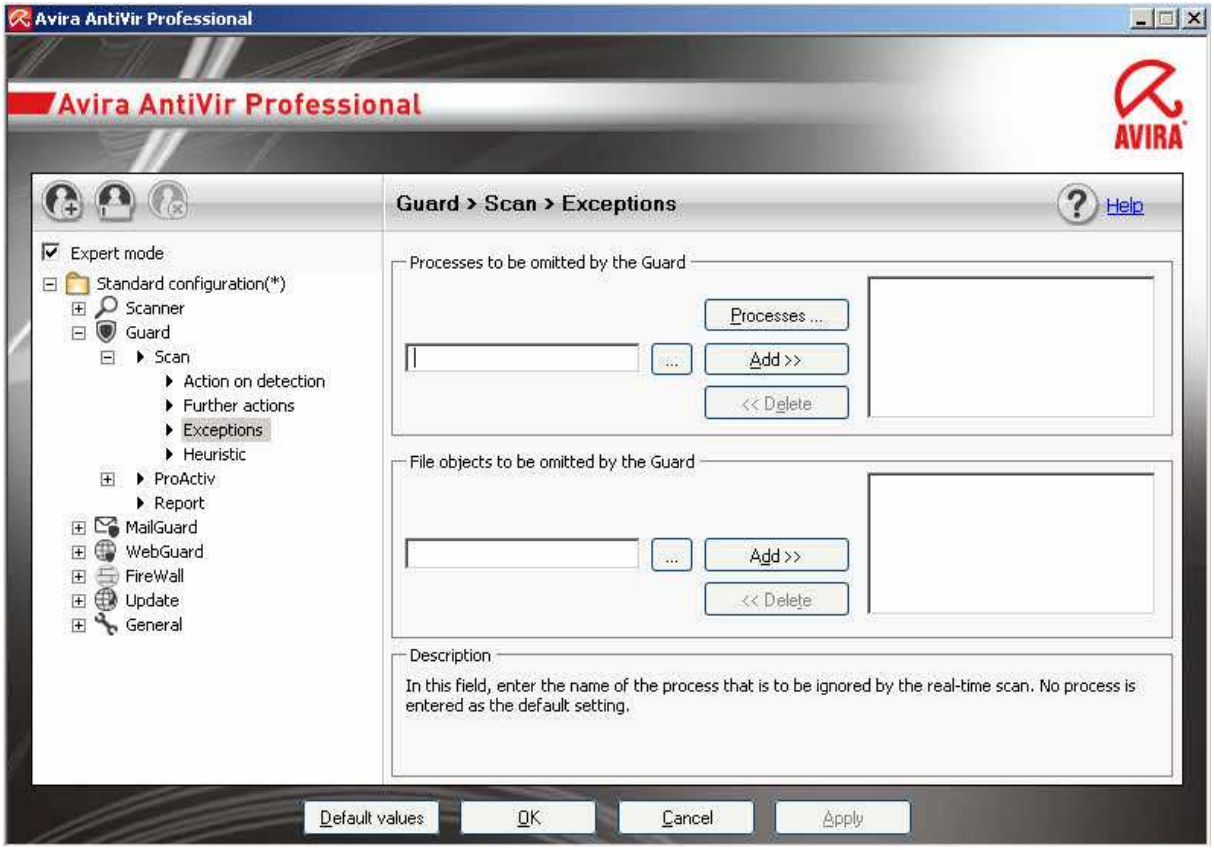
In order to prevent a slowing down of your system and exclude the concerning programs from the scan, please, proceed as follows:

- Start the configuration of the Avira AntiVir Professional
- Change to the “Expert mode”
- Open the point “Guard” and “Scan”
- Choose the point “Exceptions”

In the box “Processes to be omitted by the Guard” you have to enter the paths of the program folder where the concerned software is installed. It is important that a “\” is entered at the end of the path information so that AntiVir recognizes the path as directory and not as file.

An example for the path information:

C:\Programs\Backup_programXY\



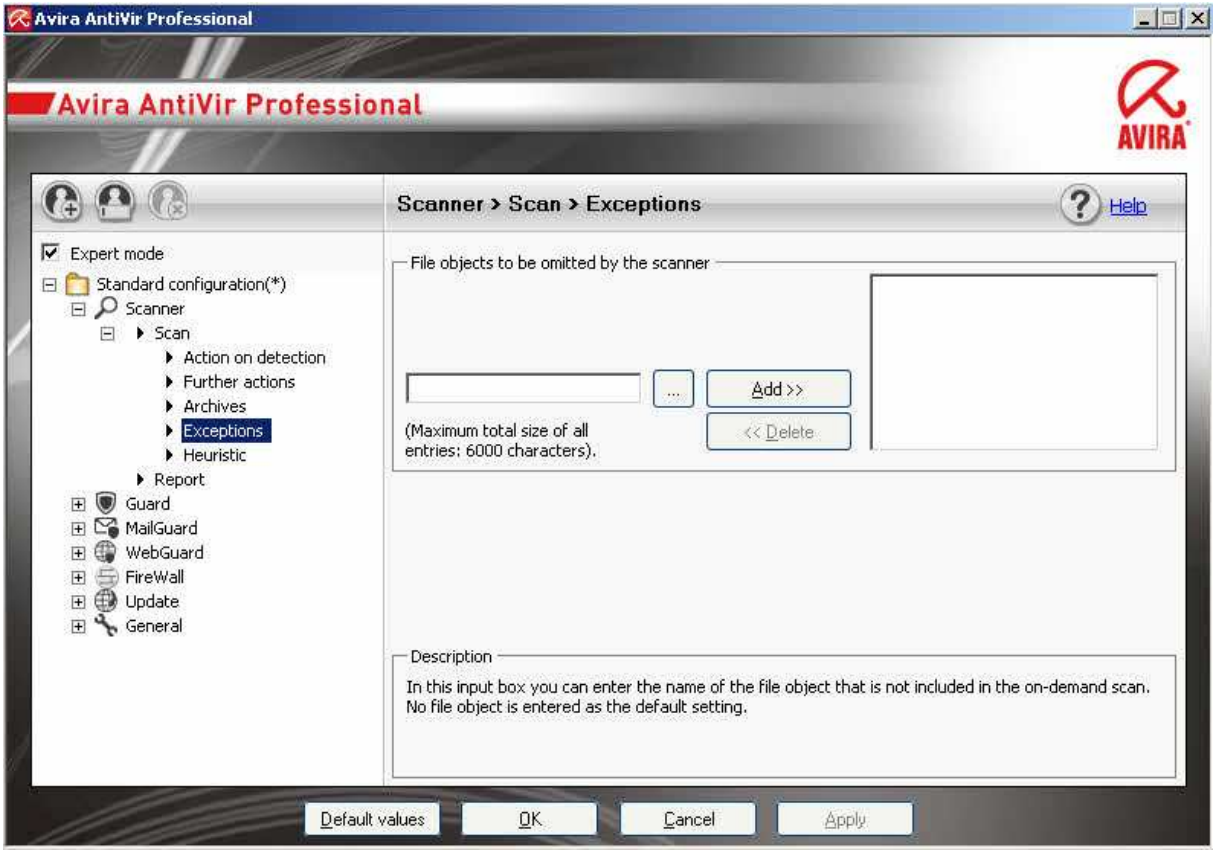
Furthermore it is important to exclude the processes of the concerning software also from the scan.

These running processes like e.g. backup software initialize accesses to files. In case the process itself is not excluded, the guard scans every read access.

So find out which processes the software uses by means of the task manager and enter them into the box “Processes to be omitted by the guard”.

In case only the program directory is omitted by the guard scan the guard will not be active in this directory. But this doesn’t concern all active processes in the task manager.

It is also important for the execution of the scan to exclude the program folders of the corresponding software from the scanner. This can be done in the menu “Scanner → Scan –> Exception”.



2.5. Configuration Profiles

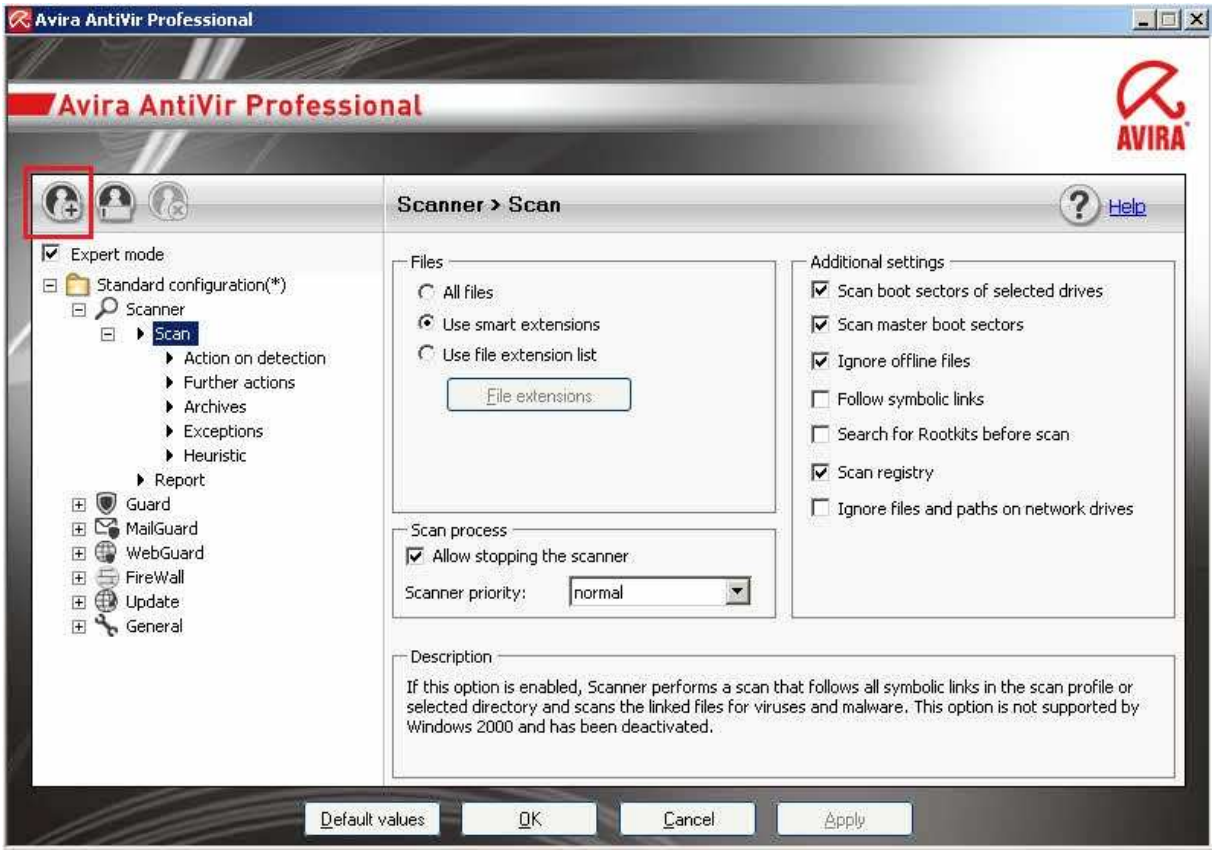
Avira AntiVir Professional offers the possibility to enter different configuration profiles. A configuration profile is a set of configuration settings which can be activated by mouse click or automatically. Configuration profiles are especially useful in enterprise networks where notebooks are used. So far, the updates for mobile devises could only be planned per default or priority server. But now you can enter two completely individual configurations.

One profile can be used in the enterprise network and another one can be active as soon as the notebook is used outside of the enterprise e.g. in the home office.

In case a proxy is used in the enterprise to load the updates or in case the WebGuard / MailGuard is not needed, you can enter the corresponding settings into a special profile. The options are changed with the profile when the notebook leaves the enterprise network.

In order to create and to configure a new configuration profile, please, proceed as follows:

- Open the configuration of the Avira AntiVir Professional
- Click on the button in the top left-hand corner for “Create new configuration” (view screenshot)
- Define a name for the profile and configure it using the expert mode



For changing the profiles you have several possibilities, so-called rules you can set. You can change the profiles manually or automatically depending on the network.

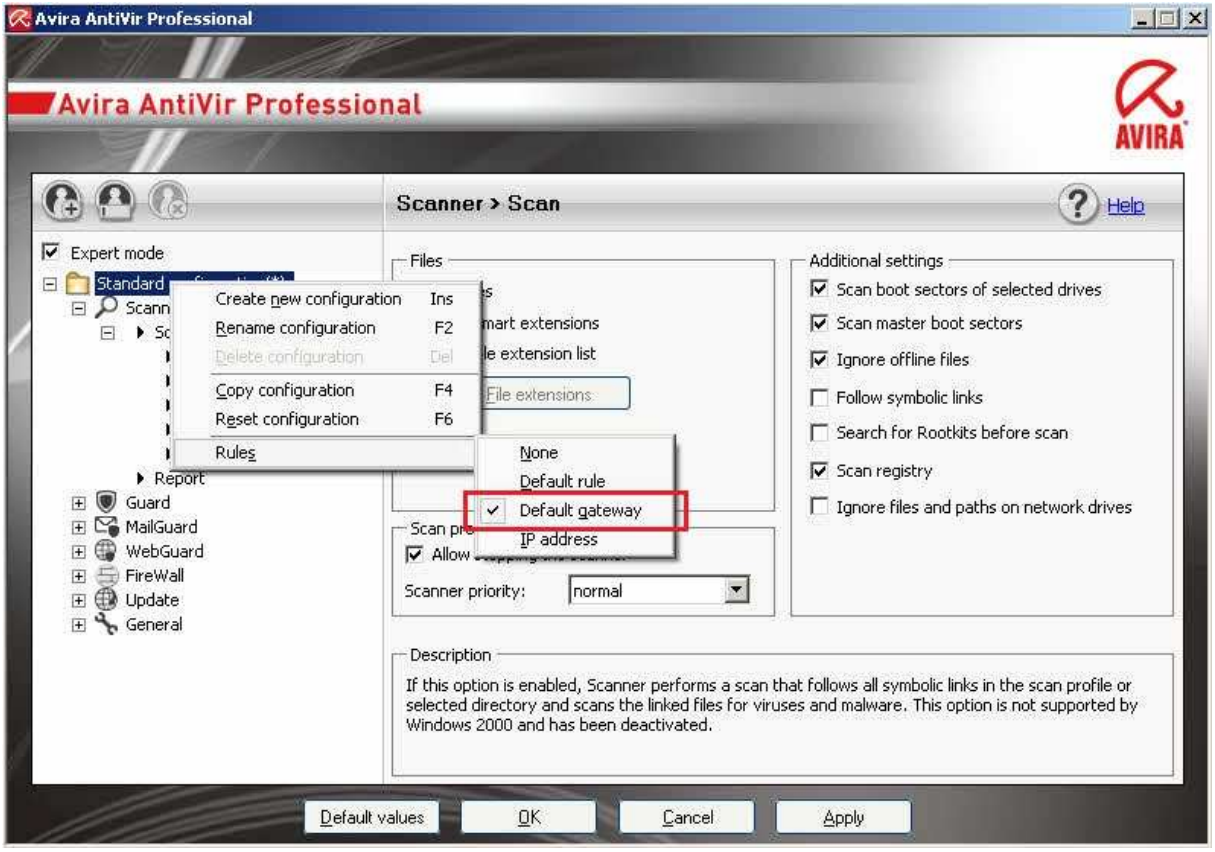
The manual change between the configuration profiles can be made via the context menu in system tray (with a right mouse click on the symbol). There you find the point “Change profile” to choose another profile.

If you want to use the automatic change you have to define a rule in the configuration of Avira AntiVir Professional. This rule defines when a special profile is activated.

In order to set the rule, click on the corresponding profile in the configuration with the right mouse button and choose the point “rule”. Here you have the following points: “None”, “Default rule” and “Default gateway”. These rules refer to the IP address of the default gateway. They are supervised by the service of the AntiVir Scheduler which changes automatically to the corresponding profile as soon as a defined rule is fulfilled.

The rule “default gateway” should always refer to the profile which is used in the in-house enterprise network. As soon as the computer is taken out of the network, the

gateway changes and Avira AntiVir Professional changes to the profile which is defined by the rule “Default gateway”.



In case a notebook is used in three different subsidiaries with different network configurations you can create three different configuration profiles and assign the profiles to the corresponding networks via a specific “Default gateway” rule.

3. Creating jobs in the scheduler

The Avira AntiVir Professional offers an integrated scheduler in order to plan one-time or regular jobs like e.g. updates and scans.

You should enter the settings for the scheduler after the installation in order to make updates and scans automatically.

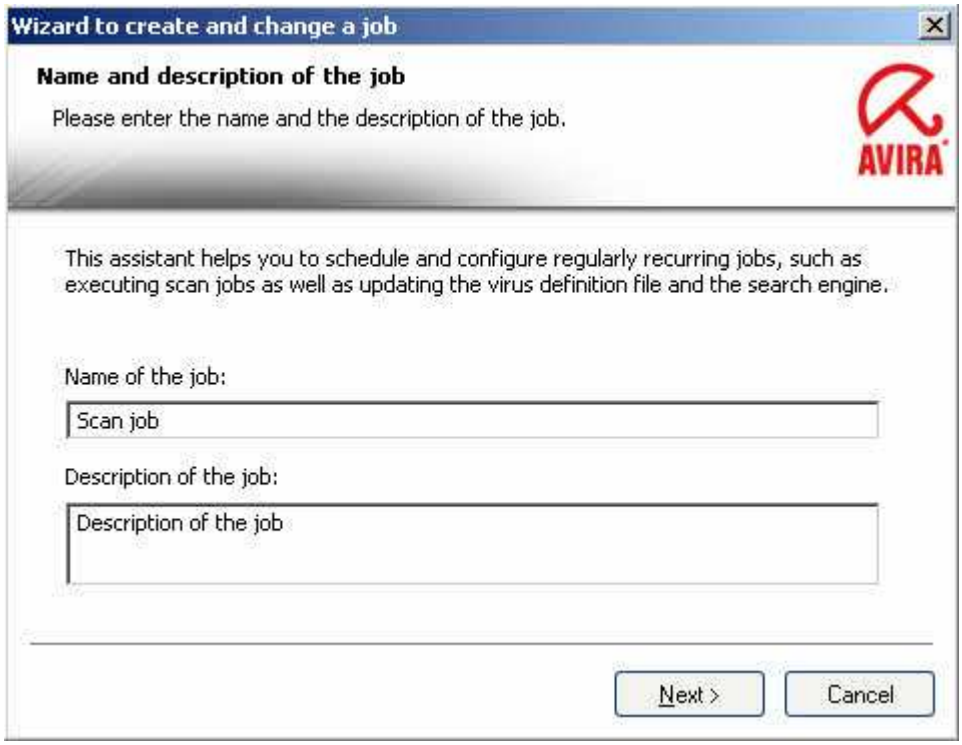
Start the AntiVir ControlCenter and choose the button “Administration” – “Scheduler”. Choose “Insert new jobs” in the toolbar. Then define a name (e.g. Internet update or weekly scan) and a short description of the job.
Enter the kind of job (in case of an update, chose “update job” and in case of a scan, choose “scan job”)

For scan jobs you can define which profile should be used for the san afterwards. You can find further information about scan profiles in chapter 4 of this document.

Then configure the point in time the job should be executed (e.g. immediately / daily / weekly / interval / single).

Afterwards you define the display mode to be used for the job. In the display mode “invisible” the whole process runs in the background. The mode “minimized” creates a small control window on the desktop which informs you about the progress of the job. The mode “maximized” creates a larger window with additional details about the running job.

Check, please, if the job is displayed as “enabled” in the overview. A checkmark has to be set in the corresponding check box.


Wizard to create and change a job
Name and description of the job
Please enter the name and the description of the job.
AVIRA
This assistant helps you to schedule and configure regularly recurring jobs, such as executing scan jobs as well as updating the virus definition file and the search engine.
Name of the job:
Scan job
Description of the job:
Description of the job
Next >
Cancel

We recommend an hourly update and a weekly scan job.

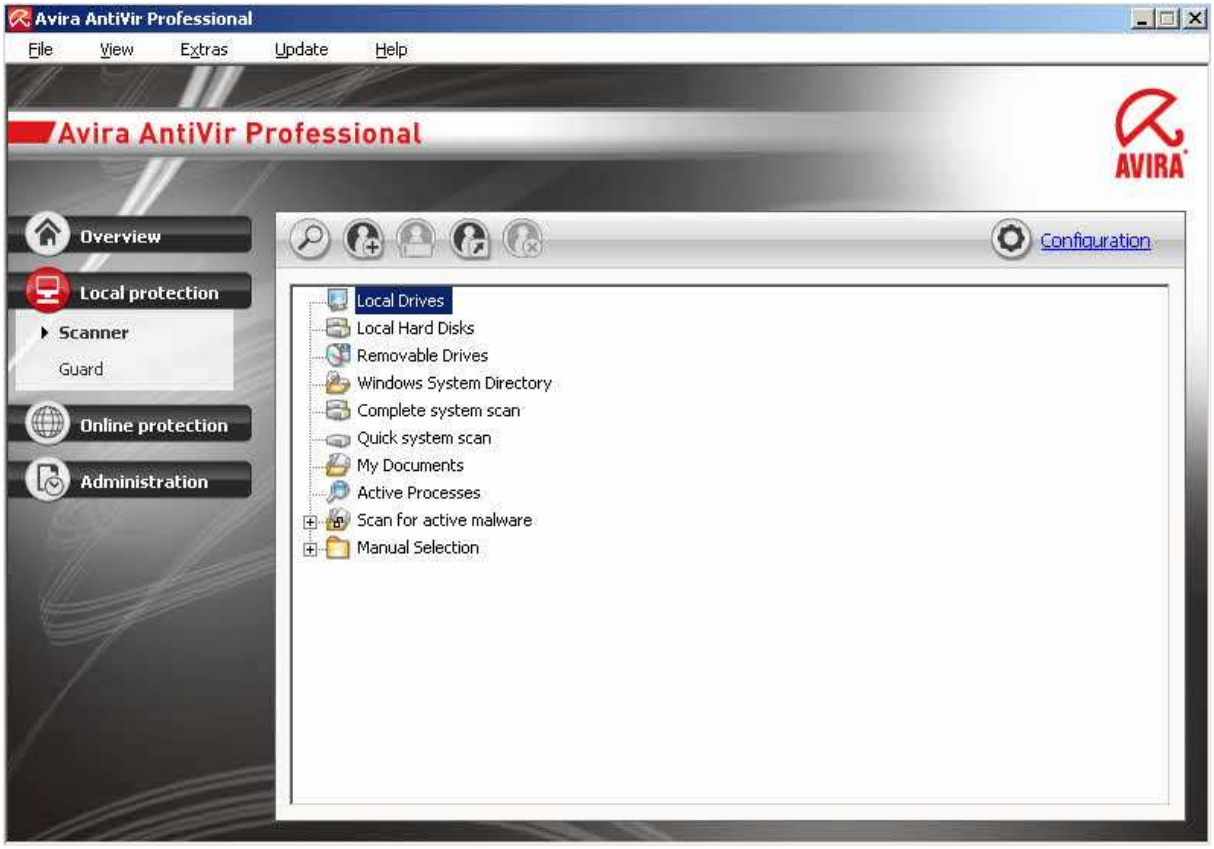
We make updates of the virus definition/engine about 5 times a day. Using hourly updates you can make sure that your protection is really up-to-date. Furthermore, the weekly system scan provides you with a maximum of security.
Frequent scans several times a day can increase your system performance. Large time periods without scans might increase the risk of viruses on the PC which could be detected after the scan.

If you make an update after a gap of several weeks or months, you could detect a virus which might have already been active for a certain time on the computer in case the AntiVir Guard hasn't already found it.
Therefore a weekly system scan is a good balance between low system load and an optimum of security of the system.

4. Different scan profiles

In case of a possible virus attack or a general control, AntiVir offers predefined scan profiles and the possibility to create individual scan profiles. By means of these profiles you can make the virus scan more effectively, so that only special sectors, drives or directories of the system are scanned.
In the following, we give you an overview of the predefined scan profiles and the possibility to adapt the scan to your individual demands.

You can find the profiles for the scan in the menu “Local protection” beneath “Scanner” in the control center of Avira AntiVir Professional.



Which scan profile is the best depends on which data have to be checked or excluded from the scan.

In case of a virus attack which can be localized on the local drives, the profile “Local drives” shortens the scan considerably. The profile “Local drives” also scans cd drives and removable media.

New unknown USB sticks which are connected to the PC should also be checked. As a complete system scan is not necessary, you can use the profile “Removable Drives” in order to make sure that there are no viruses on removable media.

In case of a virus attack, you can check if a virus is already running. The scan profile “Active Processes” looks for processes that are being processed.

The following list shows an overview of the predefined profiles and different scenarios when they should be used:

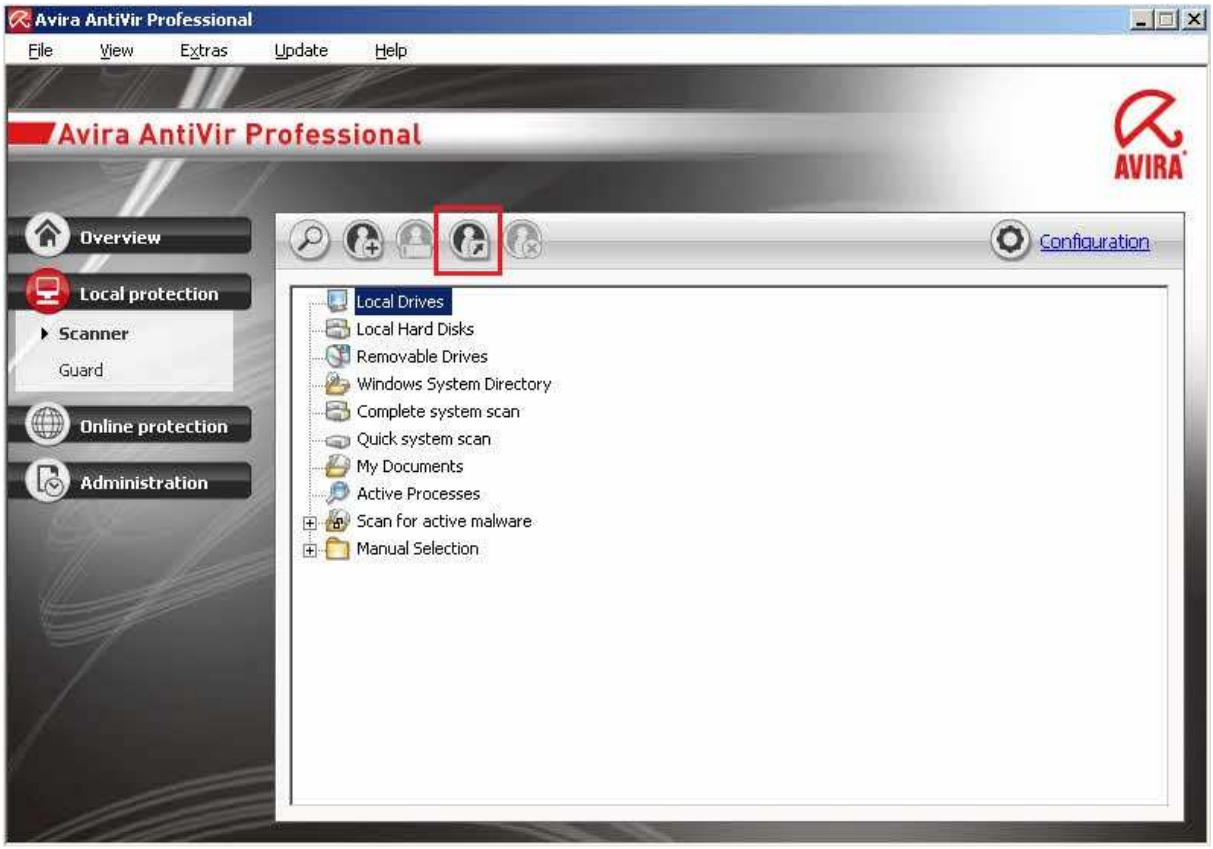
Scan profile	Explanation	Scenario
Local Drives	This profile checks all local drives.	In case you don’t know on which drive a virus is.
Local Hard Disk	This profile only checks the local hard disk on your system.	If you are sure that the virus is on the local hard disks and not on removable drives and you want to check the local hard disk directly.
Removable Drives	This profile checks all available removable drives.	If you want to make sure that a removable drive is not virulent.
Windows System Directory	Checks only the system directory of Windows (C:\Windows\System32)	If you want to make sure that the system files of Windows are clean. Many viruses write themselves into the system directory. This is a first important check if you suspect a virus attack.
Complete system scan	Makes a complete check with special scan options and will be synchronized with the GUI (server overview).	In case you don’t know if there is a virus attack and where it might be.
My Documents	Scans the folder “My Documents” of the user who is signed on.	Windows saves downloads and similar files into “My Documents” Therefore you can look here for viruses first.
Active Processes	Scans all running processes.	Check if there is a virus among the running processes.
Rootkit search	Checks the system for active rootkits. (Software which cannot be found with the usual methods of malware detections.)	This profile should be used in case of suspicion.

In order to adjust the scan for special drives and directories you can use the default profile “Manual Selection” or you can create individual scan profiles.

The manual selection or your own profiles offer you the possibility to exclude special file types from the scan or to check special file types.

Click on the corresponding scan profile with the right mouse button and choose the option “File filter”. Now you can add or delete file endings via the point “User-defined”.

You can create a desktop link for a special scan profile which allows you to start your individual scan with a click from the desktop.
You can use your created profiles in the scheduler in order to scan the directories you have defined before; e.g. a special local drive where external data is added frequently and a network drive which is connected to your PC and has to be checked.



5. Quarantine

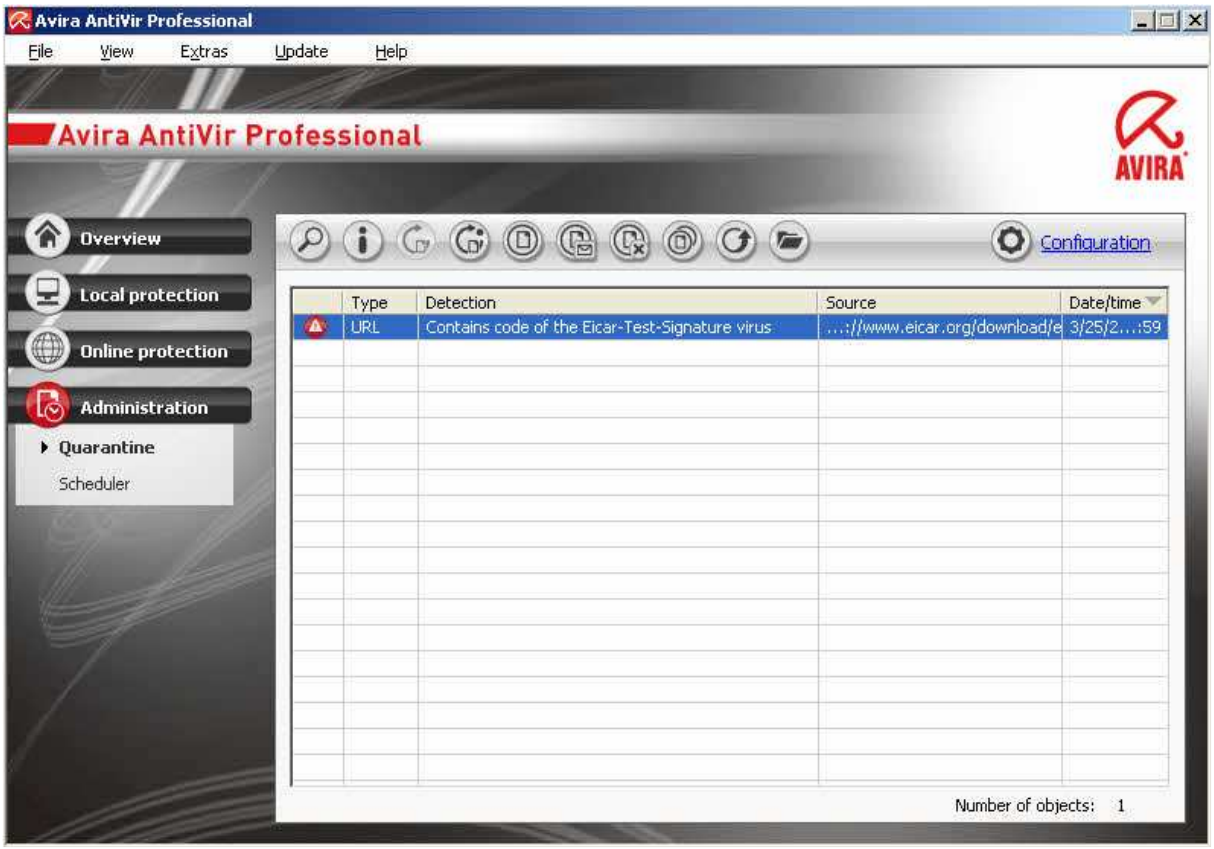
If a virus or a suspicious file is found during a scan the file is moved to the quarantine depending on the setting. The file is packed into the especially encrypted format (*.qua) and moved to the quarantine directory INFECTED on your hard disk, so that no direct access is possible any more.

This directory is located by default in case of Windows 2000/XP beneath:
C:\Documents and Settings\All Users\Application Data\Avira\AntiVir Desktop\INFECTED

For Windows Vista, the directory can be found in:
C:\ProgramData\Avira\AntiVir Desktop\INFECTED

The files in this directory can be repaired later in the quarantine manger or they can be sent to the Avira Malware Research Center, if necessary.

You can get to the quarantine administration by starting the AntiVir ControlCenter and by choosing the “Administration” – “Quarantine”.



Tip:
In the following cases, we recommend an analysis by the Avira Malware Research Center:

Heuristic Detection (suspicious files): A scan has detected a suspicious file. It has been moved to the quarantine. In the Windows dialogue of the virus detection or in the report file an analysis of the file by the Avira Malware Center has been recommended.

In case of heuristic detections the name of the detected file begins with “HEUR/…” in order to show a detection of the Advanced Heuristic Analysis and Detection (AHeAD) or ends with “.gen” if it is a generic file.
A generic detection routine is used in order to detect common characteristics of different variants.
The generic detection routine has been developed in order to detect unknown variants of already known viruses and is advanced continuously.
In case of a heuristic detection of the AHeAD the file is suspicious because of its behavior. It is possible that the file is not a virus but it might be a new unknown virus. Therefore the files should be sent to Avira for analysis.

Suspicious file: You think a file is suspicious and you moved it to the quarantine. But the check of the file for viruses and malware is negative.

False positive: You are quite sure that a detection is a false positive: Avira AntiVir Professional detects a file which is very unlikely to be malware.

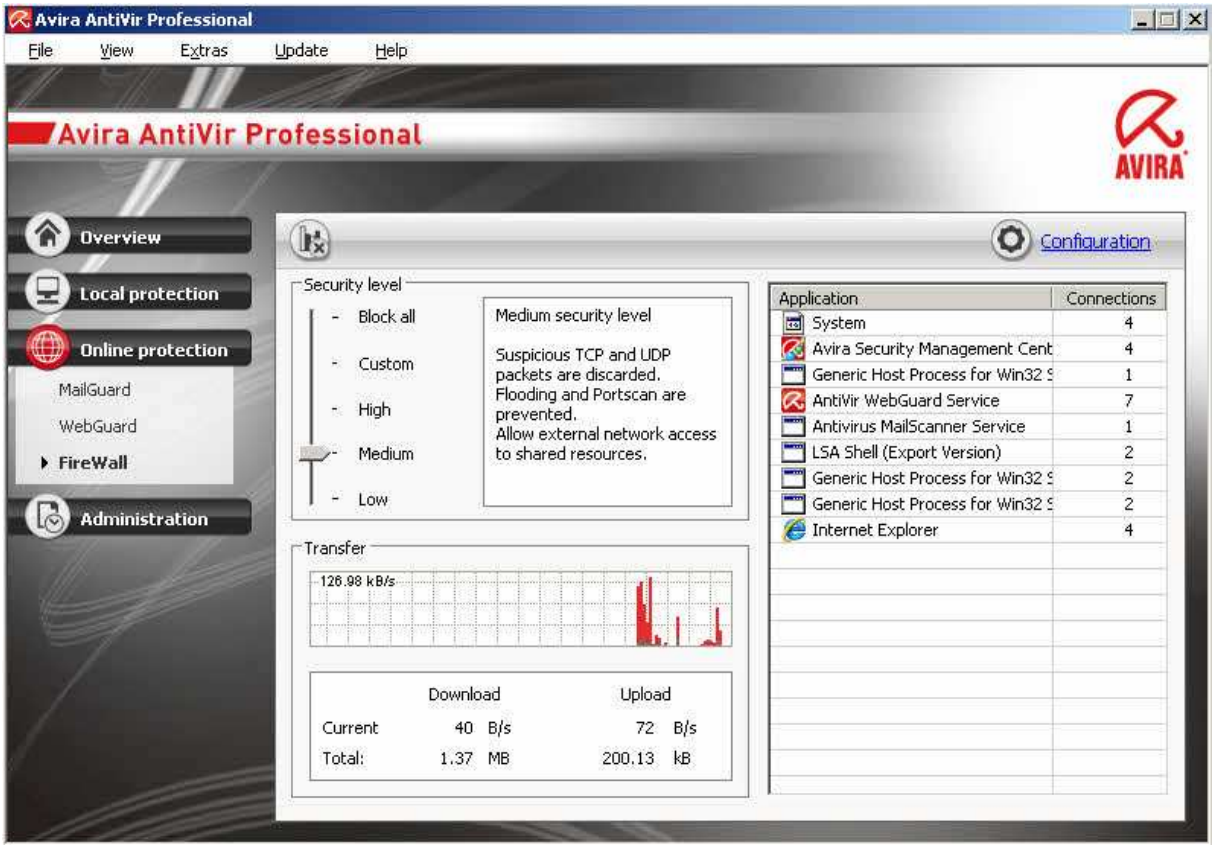
Tip
The size of the file is limited to 20 MB unpacked or 8 MB packed.

Tip
You can upload several files by marking all files you want to upload and by clicking on the button “Send object”.

You should also scan the suspicious files after a few days (between 5 and 10) with the latest virus definitions (press “F2” or right click and “Rescan object”). If the files are detected again they are very likely to be real viruses and should be deleted. If they are not detected as malware they have been false positives and can be restored.

6. Avira FireWall

A desktop firewall is integrated into the Avira AntiVir Professional 10. This component allows you to control the incoming and outgoing data traffic. On the one hand you have a scroll bar to define a security level. The security level is set on “Medium” by default. So the computer is visible in the network and file share and printer share are working.

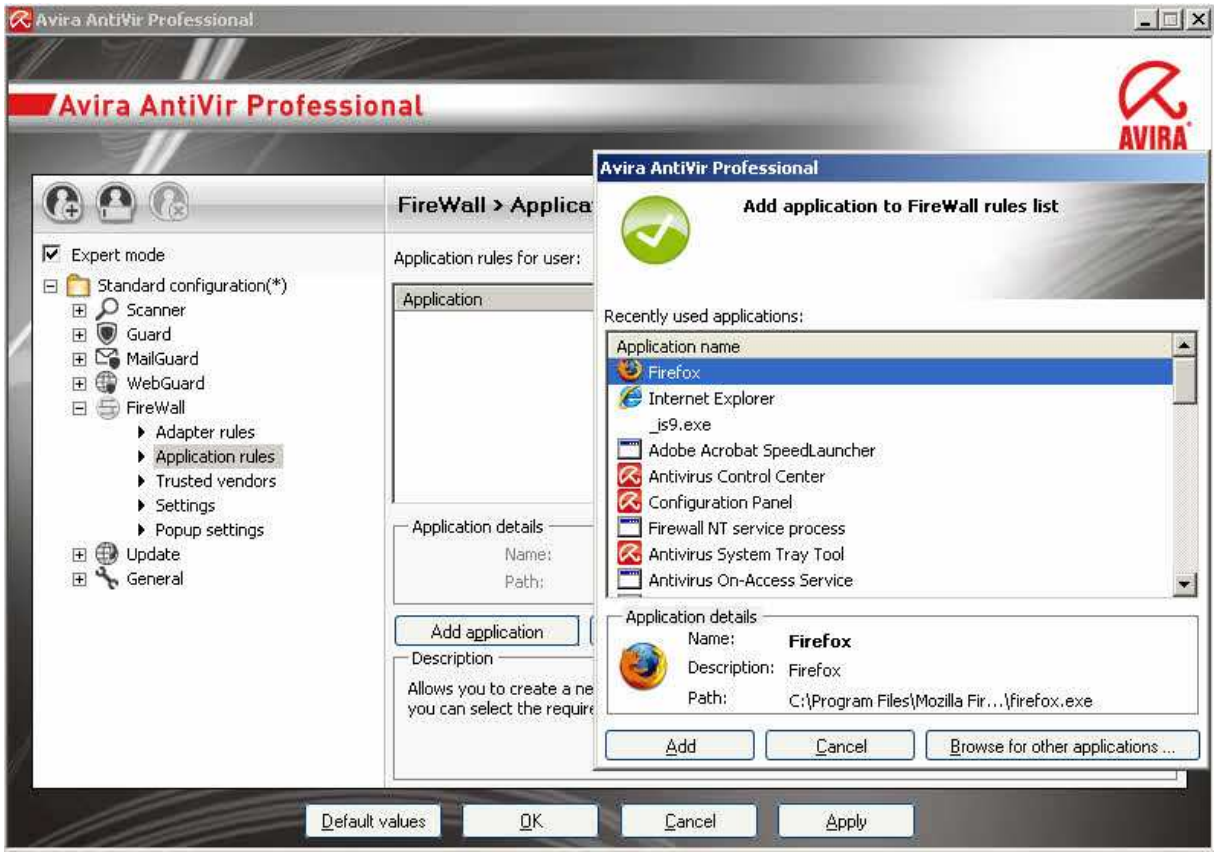


On the other hand you are provided with predefined adapter and application rules which can be individually configured and extended.

In case you want to add the browser firefox, you proceed as follows.

Open the configuration and go to “FireWall” → “Application Rules” → “Add application”.

Now a window opens and lists all applications which have been used recently. In case the application you are looking for is not shown, you can look for it by selecting “Look for further applications”:



Afterwards the application is added as a new rule and you can define how it is treated by the Avira FireWall. There are different modes or actions:

Mode:

- *Privileged:* Applications are used independently from the adapter rules or from the security level. That means the application rules are used before the adapter rules.
- *Filtered:* First the adapter rules are used and after that the application rules. In case a port should be blocked according to the adapter rules (e.g. port 80), applications can't use this port for communication (e.g. web browser).

Action:

- *Permit*: Application is allowed to communicate with the Internet
- *Deny*: Application is not allowed to communicate with the Internet.
- *Ask*: The user can select an action.

7. Quick Tips

Procedure in case of a virus attack

If the guard or the scanner should detect a virus on your system, you should scan the whole system for infected files. As many programs have exclusive read and write access on different files, a scan in the safe mode is reasonable.
You get to the safe mode by rebooting your system and by pressing F8 during the reboot. After that you choose the point “reboot in the safe mode”.

In the safe mode the AntiVir scanner receives all the necessary write accesses to all system and program files and can possibly repair files if a repair routine for the virus concerned is available.

Please make sure that the system restore of Windows is deactivated. You can deactivate it clicking on “Start” → “Programs” → “Accessories” → “System Tools”, “System Restore”.

Web-Filter of the WebGuards

The WebGuard blocks websites by default, which contain spam, malware or phishing. Furthermore fraud websites, so-called “subscription traps” are blocked as well as websites which offer a link to these sites. Here services are offered which have a low value or no value at all, but that cost a lot of money. The costs are usually hidden somewhere in the terms and conditions. Therefore the claims are not recognized according to the consumer protection.
Blocking a website can be lifted via the setting of exceptions or the deactivation of special web filter groups. Go to the configuration of the Avira AntiVir Professional, activate the expert mode and click on “WebGuard” → “Scan” → “Locked requests”. Here you see the point “Activate web filter” and the particular categories which you can choose or exclude.

LSP Reset in case of problems with the WebGuard and MailGuard

Occurring problems with the WebGuard or the MailGuard, e.g. the modules don’t start, are often caused by errors in the LSP (Layered Service Provides, a program which is in the TCP/IP socket).

It might help to uninstall the modules completely and to reset the LSP to the default values. A CMD console is needed into which “netsh winsock reset” has to be entered. Afterwards the computer has to be restarted and the MailGuard and/or WebGuard can be installed again.

Note: The registry protection has to be switched off on the computer. In case other programs should have made entries in the LSP, these entries are deleted. That means that these programs don’t work properly after a LSP reset.

An example is AVM FritzProtect which creates an entry in the LSP with the name “Sarah LSP”. Without this entry the program doesn’t work.
In order to see which entries are made in the LSP you can use e.g. the tool “sporder” which readouts the LSP stack or you execute our Support Collector on your system, which creates an image of the LSP stack.

Protocols which are checked by the MailGuard

The MailGuard offers a permanent control of your emails and checks them for viruses and malware; including the email attachments.

POP3 incoming emails are checked by default if the MailGuard is installed.

You can activate the SMTP check (outgoing emails) in the configuration of the Avira AntiVir Professional beneath “Configuration” → “MailGuard”.

The scan via the IMAP protocol is also possible. You can activate it in the configuration of the Avira AntiVir Professional clicking “Configuration” → “MailGuard” → “Monitor IMAP accounts”, In contrast to the POP3 protocol, the emails remain on the server and are administered there.

Manual insertion of the license file

If you have renewed your license and cannot load it via the button “Load license file” in the main window of the Avira AntiVir Professional, you have the possibility to copy the file (hbedv.key) directly into the main directory of AntiVir.
(C:\Program Files\Avira\AntiVir Desktop).
The result is the same as loading the file in the program via the button “Help” and “Load license file”.

Keeping the configuration for several installations

You can install the Avira AntiVir Professional on several PCs and use a defined configuration on all the PCs by means of the “avwin.ini”. You can find it in the following path:

Windows XP:
C:\Documents und Settings\All Users\Application Data\Avira\AntiVir Desktop\CONFIG\avwin.ini

Windows Vista:
C:\Programm Data\Avira\AntiVir Desktop\CONFIG\avwin.ini

You can copy this file afterwards from one PC to another and set the configuration (it is necessary to deactivate the process protection and the Avira services). Or you

enter the path to the avwin.ini via the command line during the installation e.g. in case of a logon script. The avwin.ini is imported during the installation.

In case of an automatic installation of the Avira AntiVir Professional the setup program works with the control file setup.inf. The setup program (presetup.exe) is included in the installation package of the Avira AntiVir Professional. The setup file of Avira AntiVir Professional is a self unpacking WinRAR archive which you can open and unpack with WinRAR. This archive also includes the files “presetup.exe” and “setup.inf” which are necessary for the installation in the network.
The installation is started with a script or a batch file and receives all the necessary information from the control file. The commands in the script replace the manual entries during the installation.
The Avira AntiVir Professional can be easily allocated in the network with a login script of the server or via SMC.

The following steps are necessary in order to install the Avira AntiVir Professional automatically in the network:

- Administrator rights are necessary (also in the batch mode)
- Configure the parameter of the file setup.inf and save the file
- Start the installation of Avira AntiVir Professional with the parameter /inf
- Or include the parameter into the login script of the server
  - Examples: presetup.exe /inf="c:\temp\setup.inf"
- The installation is proceeded automatically
- All entries for paths or files have to be set in “…”

Extended threat categories

Dialer programs for chargeable numbers (Dialers)
Installed on a computer these programs – shortly called dialers – guarantee the connection via a corresponding premium rate number whose pricing can be very different.
Some dialers replace the default EDI connection from the Internet user to the ISP (Internet service provider) and call for each connection a chargeable and usually very expensive 0190/0900 number.

Games
Research has shown that the working time used for computer games has reached an economically significant dimension. Therefore, more and more businesses want to keep workstations clear of games.

Jokes
Joke programs only want to scare or amuse people without being really dangerous. But be careful! Characteristics of joke programs can also originate from a virus or Trojan.

Security Privacy Risk (SPR)
Software which endangers the security of your system, doesn't proceed the desired program activities, invades your privacy or spies out your user behaviour and is therefore not wanted.

Back-door client (BDC)
In order to steal data or manipulate computers, a back-door server program is locked in via the "back-door" so that the user doesn't become aware of it. This program can be controlled by a back-door control software via the Internet or network.

Adware/Spyware
Software that displays advertising or sends the user's personal data to a third party is usually unwanted.

Unusual runtime compression
Files which have been compressed using unusual run-time compression can be regarded as suspicious.

Double-extension files
Executable files which hide their real extensions in a suspicious way can be malware.

Phishing
Phishing also known as brand spoofing, is a clever kind of data theft which targets customers or potential customers of Internet service providers, banks, online banking services and registry authorities. By entering the email address into the Internet, in an online form or in a newsgroup or website you enable so-called "Internet crawling spiders" to steal your data which is used afterwards for a fraud or other crimes.

Application (APPL)
This is an application which may pose a risk for the user and has a suspicious background.
Avira AntiVir Professional detects “Application (APPL)”. If you have chosen this option in the extended threat categories you receive a warning if Avira AntiVir Professional detects such a behavior.